Recomendaciones de Seguridad Portal Tullaveplus

En Internet se producen a diario multitud de intrusiones en sitios web, provocando en muchos casos desde simples cambios en la página principal de las páginas web (o defacement), hasta inserción de código malicioso o malware en los sistemas, creando puertas traseras que interfieren el óptimo funcionamiento del Portal. En caso de los defacement quedan visibles para todos los internautas hasta que se el administrador del sistema restituye los datos originales, incluso existen páginas de Internet que conservan el histórico de webs hackeadas y el ranking de los hackers más activos, como por ejemplo en el sitio web http://www.zone¬h.org. En años anteriores fechas como el 20 de julio o el 7 de agosto eran muy propensos los ataques a los sitios o portales web con dominios terminados en gov.co. Sin embargo se recomiendan algunas buenas prácticas adicionales a las que ya se encuentran implementadas actualmente en el portal tullave a continuación.

1. No permitir el acceso directo del root/administrador al sistema operativo

2. Asegurarse de que las contraseñas tengan caracteres en mayúscula, minúscula, con número y caracteres especiales de longitud no menor a 8 y cambiarlas regularmente.

3. Aplicar técnicas que mitiguen DDOS, como por ejemplo Modevasive para apache.

4. Configurar el Chroot: todos los usuarios no-root para mantenerlos alejados de los directorios.

5. Utilizar escáneres antivirus y filtros de spam.

6. Actualizar el software del servidor Ubuntu periódicamente.

7. Haz test de seguridad para detectar vulnerabilidades tipo pentest.

8. Intenta estar al día y estar pendientes de boletines de seguridad de Ubuntu.

9. Utilizar SSL para hacer transacciones de datos más seguras.

10. Configura los diferentes firewall con los permisos de la forma más estricta posible.

11. Evitar utilizar las mismas contraseñas para todo.

12. Realizar respaldos frecuentes de la información de base de datos, una vez al día y del filesystem del portal, una vez al mes.

13. Deshabilitar servicios innecesarios instalados en el sistema operativo.

14. No publicar el entorno de desarrollo por ningún motivo a internet.

15. Cerrar cualquier puerto de comunicación que no sea necesario

16. Configurar adicionalmente el firewall por defecto de Linux (iptables)

17. Monitorear y analizar frecuentemente los logs.

18. Configurar rotate logs para apache para poder monitorear a diario los logs.

19. Bannear ips a través de (firewall, ssh, apache, etc)

19. Revisar páginas de ips sospechosas a nivel mundial tipo http://www.abuseipdb.com.

20. Realizar hardening al Sistema operativo.

21. Monitorear disponibilidad a través de herramientas de tipo uptime como http://www.uptimerobot.com.